REMARKS/ARGUMENTS

Reconsideration and allowance of this application are respectfully requested. Currently, claims 2-8 and 23-43 are pending in this application.

Rejections Under 35 U.S.C. §103:

Claims 3, 7, 23-25, 27, 31 and 33-43 were rejected under 35 U.S.C. §103 as allegedly being unpatentable over Bachman et al (U.S. '621, hereinafter "Bachman") in view of Carlson et al (U.S. '046, hereinafter "Carlson"). Applicant respectfully traverses this rejection.

In order to establish a *prima facie* case of obviousness, all of the claim limitations must be taught or suggested by the prior art. The combination of Bachman and Carlson fails to teach or suggest all of the claim limitations. For example, the combination fails to teach or suggest the following limitations required by independent claim 23 and its dependents:

> "if an address token which uniquely re-identifies the user is contained in the client-side persistent information accompanying said request and the address token is an unvalidated address token:
>
> validating the address token using other authentication data received from the client terminal in said client-side persistent information and by reference to user authentication data already stored on said resource server;
>
> storing the validated address token for an authenticated user and an access status of the authenticated user associated with the validated address token;
>
> transmitting a client-side persistent information packet containing the validated address token to the client terminal."

Similarly, the combination to teach or suggest the following limitations required by independent claim 25 and its dependents:

> "receiving authentication data and an unvalidated identifying tag at the resource server for the user from the client terminal,

> validating said authentication data by determining if said authentication data corresponds to equivalent stored authentication details, and if so:
>
> issuing a validated identifying tag for the user to said client terminal for storage thereon;
>
> transmitting the validated identifying tag to the client terminal, the validated identifying tag being arranged to enable the client terminal to retransmit the validated identifying tag with document requests directed at said resource server; and"

The above-identified limitations relate to receiving (i) an unvalidated address token or identifying tag and (ii) authentication data at a server from a client terminal. This authentication data may be, for example, based on user name and password data. (See pg. 12, line 24 to pg. 13, line 14 of the specification). The authentication data received from the client terminal is used to determine whether the unvalidated address token (as recited in claim 23 or "unvalidated identifying tag" as recited in claim 25) which is also received from the client terminal is to be validated. The authentication data is thus used to validate (or not validate) an already existing address token (i.e., the "unvalidated address token" in claim 1 and the "unvalidated identifying tag" in claim 25).

In contrast, Bachman discloses a user at client terminal 23 transmitting a login with user identification and password to server 17. A web requestor object 211 running in server 17 receives the login request and passes it to host object 215 to verify the password with user identity information. If verified, the user identity information is passed to session object 217 which sets up a session by generating a session token from a hash of the identity information, an index and random numbers R0 and R1. (See col. 3, lines 17-38 and col. 5, lines 20-30).

Rather than use received authentication data to validate an <u>already-existing</u> address token or identifying tag also received by a server as respectively required by independent claims 23 and 25, Bachman discloses using user identity information to <u>initially generate</u> a

session token. Accordingly, Bachman fails to disclose receiving, at the server, an unvalidated address token or identifying tag and then validating this address token or identifying tag based on received authentication data. The address token and identifying tag is received and already exists at the time the authentication data is processed at the server to perform validation. Bachman discloses using the user identity information to initially generate a token. After the unvalidated address token or identifying tag is validated by the received authentication data, the validated address token or identifying tag is then transmitted back to the client terminal.

In the present invention, the resource server thus receives one type of address token or identifying tag (an unvalidated address token or identifying tag), validates this address token or identifying tag based on received authentication data, and then transmits back another type of address token or identifying tag (a validated address token or identifying tag). This is clearly not taught or suggested by Bachman which instead uses user identity information to generate an initial token. This is confirmed by Bachman's token being represented by the expression: $E_k(f(ID),R,I)$ where f(ID) is a function such as a hash function of the user's identity information. (See col. 5, lines 30-38). Again, the user identity information is used in Bachman to generate a token, not to validate a received token as claimed.

Col. 6, lines 20-50 of Bachman discloses comparing stored token information with received token information to determine if a request is to be honored based upon the stored and received token information indicating that the received token is a valid unexpired token. In particular col. 6, lines 42-49 of Bachman states "If the token is found to be invalid, or in the alternate embodiment of block 431, if the token was received from an IP address other than stored in the session table, the request is not processed by a login menu is sent to the

user at block 403 so as to determine if the user is an authorized user as was previously described with respect to these blocks 403 and 405." Blocks 403 and 405 teach generating a token based on the user identification information (as described above). Indeed, col. 5, lines 23-37 of Bachman states the following:

> "The user enters identity information such as a user ID and a memorized password that can be used to verify that the person who remembered the password is an authorized user. The user then submits the login page at block 405. At block 406, the host 19 has verified correspondence between the ID and password and at block 407, the session object 217 generates a token as described earlier with respect to FIG. 2.
>
> The token can be represented by the expression:
>
> $E_k(f(ID),R,I)$
>
> where E subscript k is the encryption using the encryption key k of the argument value in the parentheses. f(ID) is a function such as a hash function of the users identity information. R is a random number and I is the index to an entry in the session table 221."

The present invention provides the benefit of avoiding the need to perform a time-consuming verification process of the credentials of a user each time he/she seeks to access a document. Such speed is highly advantageous as users expect fast response times when accessing documents. The present invention removes the need to validate the user each time which would be very time-consuming. Instead, a validated address token or identifier is provided to the user for subsequent communications. As described above, this validated address token or identifier is obtained by validating a unvalidated address token or identifier received at the server with authentication data also received at the server. As described above, Bachman fails to teach or suggest this feature. Carlson fails to remedy this deficiency of Bachman. Accordingly, Applicant respectfully submits that the rejection under 35 U.S.C. §103 in view of Bachman and Carlson be withdrawn.

Claims 4 and 28 were rejected under 35 U.S.C. §103 as allegedly being unpatentable over Bachman, Carlson and Johnson et al (hereinafter "Johnson"). Claims 2

and 26 were rejected under 35 U.S.C. §103 as allegedly being unpatentable over the three-way combination of Bachman, Carlson and Kirsch. Claims 5, 6, 29 and 30 were rejected under 35 U.S.C. §103 as allegedly being unpatentable over the four-way combination of Bachman, Carlson, Johnson and See et al. None of these third or fourth references (Johnson, Kirsch and/or See) remedy the above-described deficiencies of the Bachman/Carlson combination. Applicant thus respectfully requests that the above-noted rejections under 35 U.S.C. §103 be withdrawn.

Conclusion:

Applicant believes that this entire application is in condition for allowance and respectfully requests a notice to this effect. If the Examiner has any questions or believes that an interview would further prosecution of this application, the Examiner is invited to telephone the undersigned.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: _____
Raymond Y. Mah
Reg. No. 41,426

RYM:sl
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4044
Facsimile: (703) 816-4100